CLAIM AMENDMENTS AND LISTING

What is claimed is:

Claim 1. (currently amended) A method for generating a key pair for use in a digital signature scheme, the method comprising:

- forming a private key which includes at least one enhancing key;~~and~~
- forming a public key which includes a commitment to said at least one enhancing key, wherein the public key and the private key form the key pair; and
- employing said key pair and said enhancing key in the generation of a digital signature.

Claim 2. (Original) The method as recited in Claim 1, wherein the step of forming a public key comprises computing a function on a commitment to an enhancing key and a 1-time public key.

Claim 3. (Original) The method as recited in Claim 1, wherein the enhancing key is randomly chosen.

Claim 4. (Original) The method as recited in Claim 1, further comprising employing the enhancing key in a process.

Claim 5. (Original) A method as recited as in Claim 4, wherein the process performs a hash calculation.

Claim 6. (Original) A method as recited in Claim 1, further comprising computing a certificate for the public key.

Claim 7. (Original) A method as recited as in Claim 1, wherein the commitment is a TCR commitment.

Claim 8. (Original) The method as recited in Claim 7, further comprising employing the enhancing key in a process.

Claim 9. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for generating a key pair, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 1.

Claim 10. (currently amended) A method of forming a TCR commitment in a digital signature scheme comprising:

- providing a commitment for a first string~~, and~~;
- applying a TCR function to a second string that includes the commitment; and
- employing said TCR commitment in the digital signature scheme.

Claim 11. (Original) A method as recited in Claim 10, wherein the step of applying includes:

- choosing a random key for the TCR function.
- evaluating the TCR function on the random key and the second string.

Claim 12. (Original) A method as recited in Claim 11, wherein the TCR function is a basic cryptographic primitive.

Claim 13. (Original) A method as recited in Claim 12, wherein the cryptographic primitive is the SHA-1 compress function.

Claim 14. (Original) A method as recited in Claim 10, wherein the step of applying forms a TCR function output which is 80 bits long.

Claim 15. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for generating a key pair, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

Claim 16. (Original) A method as recited in Claim 10, further comprising employing the TCR commitment in an enhanced commitment based signature scheme.

Claim 17. (Original) A method as recited in Claim 1, wherein the public-private key pair is used a bounded number of times.

Claim 18. (Original) A method as recited in Claim 17, where the bounded number is 36.

Claim 19. (Original) A method as recited in Claim 12, wherein the TCR function is a TCR hash tree based on a basic cryptographic primitive.

Claim 20. (Original) A method as recited in Claim 1, further comprising employing the key pair in a commitment based signature scheme.

Claim 21. (Original) The method as recited in Claim 4, wherein the process is a 36-time signature scheme.

Claim 22. (Original) A method as recited in Claim 10, further comprising employing the TCR commitment in an E-commerce protocol.

23. (currently amended) A method for generating a TCR commitment opening function, said method comprising:

generating a TCR commitment opening function for extracting a data string committed to by at least one TCR commitment message,

utilizing a corresponding TCR opening string for each said at least one TCR commitment message, and

wherein the step of generating the TCR commitment opening function includes:

receiving a TCR commitment message and the corresponding TCR opening string;

extracting a hash value and a key from said TCR commitment message; and

extracting a regular opening string and a regular commitment message from said corresponding TCR opening string,

computing the TCR hash function with said key and said regular commitment message forming a result value, and

comparing said result value with said hash value;

if the step of comparing results in a compare, applying said regular opening commitment function on said regular opening string and said regular commitment message to produce said data string.

Claim 24. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for generating a TCR commitment opening function for extracting a data string committed to by at least one TCR commitment message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 23.

Claim 25. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing generation of a TCR commitment opening function, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 23.

Claim 26. (Previously amended) A method as recited in Claim 10, wherein the step of generating the TCR commitment function includes:

receiving a data string to be committed and receiving secret information, if any, in a regular commitment scheme;

computing a regular commitment message using said regular commitment scheme upon both said data string and said secret information;

randomly selecting a key for said TCR function;

computing said TCR function on said key and said regular commitment message and obtaining a resulting hash value;

forming a TCR commitment message including said resulting hash value and said key, said TCR commitment message being an output of said TCR commitment function.

Claim 27. (Original) A method as recited in Claim 26, further comprising saving said regular commitment message.

Claim 28. (Original) A method as recited in Claim 27, wherein the step of saving is performed for a commiter.

Claim 29. (currently amended) A method used in formation of a digital signature, the method comprising:

generating a TCR de-commitment function for de-committing at least one TCR commitment message employing a TCR function and a regular commitment scheme used in generating said at least one TCR commitment message, said TCR de-commitment function used in formation of the digital signature.

Claim 30. (Original) A method as recited in Claim 29, wherein the step of generating the TCR de-commitment function includes:

receiving a data string committed and receiving secret information used in generating said at least one TCR commitment message if any;

receiving a regular commitment message computed as part of generation of said at least one TCR commitment message;

computing the regular de-commitment function on using said regular commitment message, said data string and said secret information and generating a regular opening string;

forming a TCR opening string including said regular opening string and said regular commitment message, said TCR opening string being an output of said TCR de-commitment function.

Claim 31. (currently amended) A method for generating a function used in a digital signature scheme, said method comprising:

generating a TCR commitment function by employing a TCR function and utilizing a regular commitment scheme; wherein the step of generating the TCR commitment function includes:

receiving a data string to be committed and receiving secret information, if any, in said regular commitment scheme;

computing a regular commitment message using said regular commitment scheme upon both said data string and said secret information;

randomly selecting a key for said TCR function;

computing said TCR function on said key and said regular commitment message and obtaining a resulting hash value;

forming a TCR commitment message including said resulting hash value and said key, said TCR commitment message being an output of said TCR commitment function.

Claim 32. (Canceled)

33. (Previously amended) The method as recited claim 23 wherein reporting an error if the step of comparing results in a non-compare, and reporting a non-error if the step of comparing results in a compare.

Claim 34. (Canceled)

Claim 35. (currently amended) A method for use in a digital signature scheme, said method comprising:

constructing a TCR commitment scheme comprising:

a TCR commitment function;
a TCR de-commitment function; and
a TCR commitment opening function,

by employing a TCR function and a regular commitment scheme, wherein the step of constructing the TCR commitment function includes:

receiving a data string to be committed and receiving secret information if any in said regular commitment scheme;

computing a regular commitment message using said regular commitment scheme upon both said data string and said secret information;

randomly selecting a key for said TCR function;

computing said TCR function on said key and said regular commitment message and obtaining a resulting hash value; and forming a TCR commitment message including said resulting hash value and said key, said TCR commitment message being an output of said TCR commitment function.

Claim 36. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for generating a TCR commitment function, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the step of claim 25.

Claim 37. (Original) A method as recited in Claim 25, wherein the TCR function is a basic cryptographic primitive.

Claim 38. (Original) A method as recited in Claim 37, wherein the cryptographic primitive is the SHA-1 compress function.

Claim 39. (Original) A method as recited in Claim 26, wherein said resulting hash value is 80 bits long.

Claim 40. (Original) A method as recited in Claim 25, wherein the TCR function is a TCR hash tree based on a basic cryptographic primitive.

Claim 41. (Original) A method as recited in Claim 35, further comprising employing the TCR commitment scheme in an enhanced commitment based signature scheme.

Claim 42. (Original) A method as recited in Claim 35, further comprising employing the TCR commitment scheme in an E-commerce protocol.

Claim 43. (Previously amended) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing formation of a TCR commitment message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 31.

Claim 44. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for generating a TCR de-commitment function, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 29.

Claim 45. (new) A method for generating a key pair, the method comprising:

- forming a private key which includes at least one enhancing key; and
- forming a public key which includes a commitment to said at least one enhancing key, wherein the public key and the private key form the key pair.

Claim 46. (new) A method of forming a TCR commitment comprising:

- providing a commitment for a first string, and
- applying a TCR function to a second string that includes the commitment.

Claim 47. (new) A method comprising:

generating a TCR de-commitment function for de-committing at least one TCR commitment message employing a TCR function and a regular commitment scheme used in generating said at least one TCR commitment message.